2. Polynomial rings

Let \( R \) be a ring. A polynomial in one variable over \( R \) is

\[
F(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n,
\]

where \( a_i \in R \) and \( a_i = 0 \) for all but finitely many \( i \). If \( a, b \in P(R) \), define operations:

\[
a + b = (a_i + b_i)
\]

\[
a b = (\sum_{j=0}^{\infty} a_j b_{i-j}) = (a_0b_0, a_0b_1 + a_1b_0, a_0b_2 + a_1b_1 + a_2b_0, \ldots)
\]

**Thm 2.1**: If \( R \) is a ring, then \( P(R) \) is a ring. It is commutative iff \( R \) is, and it has 1 iff \( R \) does, in which case \( 1_{P(R)} = (1, 0, 0, 0, \ldots) \)

**Pf**: Exercise.

Let \( R \) be a ring with 1, set \( x = (0, 1, 0, 0, \ldots) \in P(R) \).

**Note**: \( x^2 = (0, 0, 1, 0, 0, \ldots) \), \( x^3 = (0, 0, 0, 1, 0, 0, \ldots) \), etc.

Say \( x^0 = 1_{P(R)} \). The map \( a \mapsto (a, 0, 0, \ldots) \) is a monom.

\( R \to P(R) \). Thus we may identify \( R \) with a subring of \( P(R) \), \( 1_R = 1_{P(R)} \). Now, we may write

\[
a = (a_0, a_1, a_2, \ldots) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \ldots
\]

for each \( a \in P(R) \).

Call \( x \) an indeterminate, and write \( R[x] = P(R) \).
Write \( f(x) \) for \( x \in R[x] \), called a polynomial with coefficients in \( R \). If \( a_n \neq 0 \), but \( a_n = 0 \) for all \( n > n \), say \( f(x) \) has degree \( n \), and leading coefficient \( a_n \). If \( f(x) \) has leading coefficient \( 1 \), call \( f(x) \) monic. Call the zero polynomial \( (0, 0, 0, \ldots) \), denoted by \( 0 \). Say \( \deg 0 = -\infty \).

Polynomials of degree 0 or \(-\infty\) are constants (elts of \( R \)).

Prop 2.2: Let \( R \) be a ring with \( 1 \) and \( f(x), g(x) \in R[x] \). Then

(a) \( \deg (f(x) + g(x)) \leq \max \{ \deg f(x), \deg g(x) \} \), and

(b) \( \deg (f(x)g(x)) \leq \deg f(x) + \deg g(x) \).

Moreover, equality holds in (b) if \( R \) has no zero divisors.

\[ \text{Pf: Exercise.} \]

Cor 1: If \( R \) has no zero divisors, then \( f(x) \in R[x] \) is a unit iff \( f(x) = r \) with \( r \in U(R) \).

Cor 2: \( R[x] \) is an integral domain iff \( R \) is an integral domain.

Thm 2.3: (Division algorithm). Suppose \( R \) is commutative with \( 1 \) and \( f(x), g(x) \in R[x] \). If \( g(x) \) has leading coeff. \( b \), then there exists \( k \geq 0 \) and \( q(x), r(x) \in R[x] \) such that

\[ b^k f(x) = q(x) g(x) + r(x), \text{ with } \deg r(x) < \deg g(x). \]

If \( b \) is not a zero divisor in \( R \), then \( q(x) \) and \( r(x) \) are unique, if \( b \in U(R) \) we may take \( k = 0 \).
Proof: If \( \deg f(x) < \deg g(x) \), we may take \( k=0, \ g(x)=0, \) and \( r(x)=f(x) \). Thus, assume that \( \deg f(x) = m > \deg g(x) = n, \) and \( f(x) = a_0 + a_1 x + \cdots + a_m x^m, \ g(x) = b_0 + b_1 x + \cdots + b_n x^n, \) and set \( a := a_m \) and \( b := b_n \) for clarity.

Induct on \( m \). Base case trivial.

Assume it's true for polynomials of degree \( < m \).

Set \( f_1(x) = b f(x) - a x^{n-m} g(x) \).

Clearly, \( \deg f_1(x) < m \), so we may write

\[
\begin{align*}
b^{k-1} f_1(x) &= p(x) g(x) + r(x) \quad \text{where} \quad \deg r(x) < \deg g(x). \\
b^k f(x) &= b^{k-1} b f(x) = b^{k-1} \left( a x^{n-m} g(x) + f_1(x) \right) \\
&= b^{k-1} a x^{n-m} g(x) + b^{k-1} f_1(x) \\
&= b^{k-1} a x^{n-m} g(x) + p(x) g(x) + r(x) \\
&= \left( b^{k-1} a x^{n-m} + p(x) \right) g(x) + r(x) \quad \checkmark
\end{align*}
\]

Call this \( q(x) \).

Next, suppose \( b \) is not a zero divisor, and

\[
\begin{align*}
b^k f(x) &= q_1(x) g(x) + r_1(x), \quad \text{and} \\
b^k f(x) &= q_1(x) g(x) + r_1(x). \quad \text{with} \quad \deg r(x), r_1(x) < \deg g(x).
\end{align*}
\]

Then, \( (q_1(x) - q_1(x)) g(x) = r_1(x) - r(x) \).

If \( q(x) \neq q_1(x) \), then the LHS has degree \( \geq n \), since the leading coeff. of \( g(x) \) is \( b \) (not a zero divisor).
However, the RHS has degree \( n < m \).

Thus, \( q(x) = q_1(x) \), and \( r(x) = r_1(x) \).

Finally, if \( b \in U(R) \), multiply \( \phi(\theta(x)) \) by \( b^{-k} \), and replace \( q(x) \) \( r(x) \) by \( b^{-k}q(x) \) \( b^{-k}r(x) \), resp. 

The polynomials \( q(x) \) and \( r(x) \) are called the quotient and remainder.

The division algorithm also holds when \( R \) is not comm, as long as \( b \) is a unit.

Henceforth, \( R \) is assumed to be commutative with \( 1 \).

**Thm 2.4.** (Substitution). Suppose \( R, S \) comm. rings with \( 1 \), that \( \theta : R \rightarrow S \) is a homom. with \( \theta(1_R) = 1_S \) and \( a \in S \). Then \( \exists ! \) homom \( E_a : R[x] \rightarrow S \) s.t.

1. \( E_a(r) = \theta(r) \) \( \forall r \in R \)
2. \( E_a(x) = a \).

"Maps \( f(x) \) to \( f(a) \)."

**Pf:** It is easy to show that \( E_a \) is a homom if \( E_a(r) = \theta(r) \).

**Uniqueness:** Suppose \( F : R[x] \rightarrow S \) is a homom with \( F(r) = \theta(r) \) \( \forall r \in R \) and \( F(x) = a \). Then

\[
F(f(x)) = F(\sum_{i=0}^{n} r_i x^i) = F(r_0) + F(r_1)F(x) + \ldots + F(r_n)F(x^n)
\]

\[
= \theta(r_0) + \theta(r_1)a + \ldots + \theta(r_n)a^n
\]

\[
= E_a(f(x))
\]
Examples:

\[ \mathbb{Z} \xrightarrow{\Phi} \mathbb{Z}[x] \]

\[ \mathbb{Z} \xrightarrow{\Theta} \mathbb{R} \]

\[ \mathbb{R} \xrightarrow{E_{\sqrt{2}}} \mathbb{Z}[\sqrt{2}] \]

\[ \mathbb{Z} \xrightarrow{\Phi} \mathbb{Z}[x] \]

\[ \mathbb{Z} \xrightarrow{\Theta} \mathbb{C} \]

\[ \mathbb{C} \xrightarrow{E_i} \mathbb{R} \]

**\( \Phi \):** \( f(x) \mapsto f(\sqrt{2}) \).

Image is the subring \( \mathbb{Z}[\sqrt{2}] \subseteq \mathbb{R} \) generated by elts \( a+b\sqrt{2} \) for \( a, b \in \mathbb{Z} \).

Note: \( \mathbb{Z}[\sqrt{2}] = \{ a + b\sqrt{2} : a, b \in \mathbb{Z} \} \) (Why?)

**\( \Theta \):** \( f(x) \mapsto f(i) \).

Image is the subring \( \mathbb{Z}[i] \subseteq \mathbb{C} \); all elts of the form \( a+bi \) for \( a, b \in \mathbb{Z} \) (called the Gaussian integers).

The map \( \Phi \) is called the evaluation map at \( \alpha \).

Note: \( \Theta \) need not be an injection, but in practice, it is usually the canonical inclusion map. In this case, \( \Phi_\alpha(f(x)) = r_0 + r_1a + \ldots + r_na^n \), which we call \( f(x) \), and we write the image as \( R[\alpha] = \{ f(x) : f(x) \in R[x] \} \).

**Prop 2.5 (Remainder Theorem).** Suppose \( R \) is comm. with 1, \( f(x) \in R[x] \), and \( \alpha \in R \). Then the remainder of \( f(x) \) divided by \( g(x) = x-\alpha \) is \( r = f(\alpha) \).

**PF:** Write \( f(x) = g(x)(x-\alpha) + r \). Substitute \( \alpha \) for \( x \) to get \( f(\alpha) = g(\alpha)(\alpha-\alpha) + r = r \). \( \square \)
Cor. (Factor theorem): Suppose $R$ is comm. with 1, $f(x) \in R[x]$, $a \in R$ and $f(a) = 0$. Then $x-a$ is a factor of $f(x)$, i.e., $f(x) = g(x)(x-a)$ for some $g(x) \in R[x]$.

Def: If $R \subseteq S$ are comm. rings with $R \subseteq S$, $1_R = 1_S$, then an elt $a \in S$ is algebraic over $R$ if $f(a) = 0$ for some non-zero polynomial $f(x) \in R[x]$. If $a \in S$ is not algebraic over $R$, it is transcendental over $R$.

Note: $a \in S$ is algebraic over $R$ iff $E_a$ is not 1-1.

Example: $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Z}$ since $f(\sqrt{2}) = 0$ for $f(x) = x^2 - 2$.

$\pi \in \mathbb{R}$ is transcendental over $\mathbb{Z}$.

If $R$ is an integral domain, then the field of fractions of $R[x]$ is the field of rational functions over $R$:

$$R(x) = \{ \frac{f(x)}{g(x)} : f(x), g(x) \in R[x], \ g(x) \neq 0 \}.$$ 

Polynomials in several indeterminates,

Let $I = \{0,1,2,3,...\}$ and consider $I^n = I \times ... \times I$ ($n$ copies).

Let $R$ be a ring, and define

$$P_n(R) = \{ a : I^n \to R : a(x) = 0 \text{ all but finitely many } x \in I^n \}.$$ 

Note: If $n=1$, then $P_1(R) = P(R)$.

Write $0$ for $(0,0,...,0) \in I^n$ and if $i = (i_1, i_2, ... , i_n) \in I^n$ and $j = (j_1, j_2, ... , j_n) \in I^n$, define

$$i \cdot j = (i_1j_1, i_2j_2, ... , i_nj_n) \in I^n.$$
Define addition and multiplication on $P_n(R)$ as follows:

$$(a+b)(i) = a(i) + b(i)$$
$$(ab)(i) = \sum \{a(j)b(k) : j, k \in I^n, j + k = i\}$$

Informally, think of an elt of $I^n$ as corresponding to a monomial. E.g., $a(0, 3, 4) = -6 \leftrightarrow -6x_1^0x_2^3x_3^4$, and a function in $P_n(R)$ as assigning coefficients to monomials.

**Theorem 2.6:** If $R$ is a ring, then $P_n(R)$ is a ring, and $P_n(R)$ is comm. iff $R$ is, and has 1 iff $R$ has 1.

**Proof:** Exercise (straightforward, but tedious).

**Note:** The identity function $1 \in P_n(R)$ is the function $1 : soln \mapsto R$, where $1(0) = 1 \in R$, $1(i) = 0 \in R$ if $0 \neq i \in I^n$.

(Secretly, assigns coeff. 1 to $x_1^0x_2^0...x_n^0$, 0 otherwise.)

For each $r \in R$, define a function $a_r \in P_n(R)$:

$a_r(0) = r$, $a_r(i) = 0$ if $0 \neq i \in I^n$.

Then, $a_r + a_s = a_{r+s}$ and $a_r a_s = a_{rs}$.

So, the map $r \mapsto a_r$ (secretly, $r \mapsto rx_1^0x_2^0...x_n^0$) is 1-1.

Thus, we may identify $r$ with $a_r \in P_n(R)$, and view $R$ as a subring of $P_n(R)$.

Let $R$ be a ring with 1, let $E_k = (0, 0, ..., 0, 1, 0, ..., 0)$

Define $X_k \in P_n(R)$: $X_k(E_k) = 1$, $X_k(i) = 0$ if $E_k \neq i \in I^n$.

Often, if $n = 2, 3$, write $X_1 = X$, $X_2 = Y$, $X_3 = Z$.
Note: \( x_k^2(2e_k) = 1, \ x_k^2(i) = 0 \ i \neq 2e_k \), and in general, 
\( x_k^n(me_k) = 1, \ x_k^n(i) = 0 \ i \neq me_k \) for \( 1 \leq m \leq 2 \).

[secretly, e.g., \((0, 3, 0) \mapsto 1 x_1^2 x_2^3 x_3^0 = 1 x_2^3\).]

Note: \( x_i \cdot x_j = x_j \cdot x_i \) (i.e., these commute as functions, \( \mathbb{R}^n \to \mathbb{R} \)).

For any \( i \in \{i_1, \ldots, i_n\} \in \mathbb{I}^n \) and \( r \in \mathbb{R} \), consider \( rx_1^{i_1} \cdots x_n^{i_n} e_{P_n}(R) \), which has value \( r \) at \( i \in \mathbb{I}^n \) and 0 elsewhere, i.e., has one-point support.

Since any \( a \in \mathbb{P}_n(R) \) can be written uniquely using functions with one-point support, each \( 0 \neq a \in \mathbb{P}_n(R) \) can be written uniquely as a sum of elts of the form \( rx_1^{i_1} \cdots x_n^{i_n} \), called monomials.

Say that the degree of \( a = rx_1^{i_1} \cdots x_n^{i_n} \) is \( \deg a = i_1 + \ldots + i_n \).

If \( a \) is a sum of monomials \( a = a_1 + \cdots + a_m \), then say
\( \deg a = \max \{ \deg a_i : 1 \leq i \leq m \} \).

Also, say that \( \deg 0 = -\infty \), and if all \( a_i \)'s have the same degree, call \( a \in \mathbb{P}_n(R) \) homogeneous.

The elements of \( \mathbb{P}_n(R) \) are called polynomials in the \( n \) commuting indeterminates \( x_1, \ldots, x_n \).

We write \( R[x_1, \ldots, x_n] \) for \( \mathbb{P}_n(R) \) and denote elements by \( f(x_1, \ldots, x_n) \), etc.

Often, we write \( X \) for \( (x_1, \ldots, x_n) \) and then \( f(X) \) for \( f(x_1, \ldots, x_n) \).
Prop 2.7: Let \( R \) be a ring with 1 and \( f(x), g(x) \in R[x_1, \ldots, x_n] \). Then:
(a) \( \deg(f(x) + g(x)) \leq \max \{ \deg f(x), \deg g(x) \} \),
(b) \( \deg(f(x)g(x)) \leq \deg f(x) + \deg g(x) \).

Moreover, equality holds in (b) if \( R \) has no zero divisors.

Thm 2.8: (Substitution). Let \( R, S \) be comm. rings with 1, and \( \Theta: R \to S \) a homom with \( \Theta(1_R) = 1_S \). If \( a_1, \ldots, a_n \in S \), then \( \exists! \) homom
\[
E = E_{(a_1, \ldots, a_n)}: R[x_1, \ldots, x_n] \to S
\]

s.t. (i) \( E(r) = \Theta(r) \) \( \forall r \in R \)
(ii) \( E(x_i) = a_i \); \( 1 \leq i \leq n \)

Proof: Define \( E(r, x_1, \ldots, x_n) = \Theta(r) a_1, \ldots, a_n \). For monomials, extend to polynomials in the obvious way. Check this works. \( \square \)

Note: We could have defined \( R[x_1, \ldots, x_n] \) abstractly using this universal mapping property.

Another construction: Define \( R[x_1, x_2] = (R[x_1])[x_2] \), etc.

We could extend this to an arbitrary index set as well, i.e., define \( R[x_a : a \in A] \).

If \( \Theta \) is injective, then the homom. \( E \) "substitutes" elements from \( S \) in place of the \( x_i \)'s, by \( f(x_1, \ldots, x_n) \mapsto F(a_1, \ldots, a_n) \)

where \( a_i \in S \).

The image is a subring of \( S \), denoted \( R[a_1, \ldots, a_n] \).
Example:

\[ \mathbb{Z} \rightarrow \mathbb{Z}[x, y] \rightarrow \mathbb{R} \]

\[ \text{In}(E) = \mathbb{Z}[\sqrt{3}, \sqrt{5}] = \{a + b\sqrt{3} + c\sqrt{5} + d\sqrt{15} : a, b, c, d \in \mathbb{Z}\} \]

Def: Elements \( a_1, \ldots, a_n \in S \) are algebraically dependent over \( R \)
if \( f(a_1, \ldots, a_n) = 0 \) for some \( 0 \neq f(\bar{x}) = R[x_1, \ldots, x_n] \).
Otherwise, they are algebraically independent over \( R \).

Ex: (1) \( a_1 = \sqrt{3}, a_2 = \sqrt{5} \) are algebraically dependent over \( \mathbb{Z} \)
consider \( f(x, y) = (x^2 - 3)(y^2 - 5) \)
(2) \( a_1 = \sqrt{n}, a_2 = 2\pi + 1 \) are algebraically dependent over \( \mathbb{Z} \)
consider \( f(x, y) = 2x^2 - y + 1 \)
(3) It is unknown whether \( a_1 = \pi, a_2 = e \) are algebraically dependent over \( \mathbb{Z} \).

Note: 
- \( a \in S \) algebraically independent over \( R \) \( \iff \) \( a \) transcendental over \( R \).
- \( a_1, \ldots, a_n \) alg. indep. over \( R \) \( \rightarrow \) all \( a_i \) transcendental over \( R \).

"\( \iff \)" fails (See Ex. (2) above).

Usually, we omit \( x_1^0 \), so \( R[x_1] \subseteq R[x_1, x_2] \subseteq R[x_1, x_2, x_3] \subseteq \ldots \)
and write \( R[x_1, x_2, x_3, \ldots] := \bigcup \{ R[x_1, \ldots, x_k] : 1 \leq k \in \mathbb{Z} \} \).

If \( R \) is an integral domain, then the field of fractions of \( R[x_1, \ldots, x_n] \) are the rational functions (denoted \( R(x_1, \ldots, x_n) \))
\[ \left\{ \frac{f(x_1, \ldots, x_n)}{g(x_1, \ldots, x_n)} : g(x_1, \ldots, x_n) \neq 0, f(x_1, \ldots, x_n), g(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n] \right\} \]